DIGITAL CURRENCY IN THE CURRENT CYBER SECURITY ENVIRONMENT

PhD Student Radu BORES
"Ştefan cel Mare" University of Suceava, Romania
Email: radu.bores@gmail.com
PhD Assistant Ana Maria HLACIUC
"Ştefan cel Mare" University of Suceava, Romania
Email: hlaciuc_anamaria@yahoo.com

Abstract: *This paper presents a view over the development of new technologies and infrastructures that lead to the rise of decentralized digital currencies such as Bitcoin. In the context of an evolving cyber security environment and increasing dependence on computer systems, such solutions present not only interesting applications, but also challenges to developers, regulators and even users. We analyze several financial applications branching out of this technology and various derivatives from the initial developments, such as smart contracts. Also, we look at several limitations that have to be addressed in order for these technologies to be sustainable for the future and succeed.*

Keywords*: cryptocurrency, bitcoin, decentralization, block - chain, financial infrastructure.*
JEL Classification: *P34, P24, E59.*

1. Introduction

With the advance of technology and the rise in complexity of the systems and technical mechanisms underlying the functioning of modern society, a new form of security became essential, that applied to all computational devices: computers, networks, digital electronic equipment. Cybersecurity has both physical and digital relevance, namely to protect the integrity of equipment and circuits, protecting data and information stored, transferred or processed by equipment and physical facilities. Due to the increasing dependence on computer systems, a range of vulnerabilities in a variety of sectors are relevant: financial systems, utilities, industrial equipment, personal consumer devices, IT infrastructure of companies or even governments. Effective Cybersecurity is its ability to protect against unauthorized access, alteration or destruction of equipment, theft information or affecting privacy and data integrity.

Cybercrime is one of the most significant categories, both due to increase from year to year and the huge volume of annual losses. As society uses technology more extensively for storing wealth and digitally quantifying value (currencies, investment accounts and savings, stocks, bonds and other financial instruments, pensions) all the vulnerabilities of these systems are becoming a serious concern for governments, companies and even individuals. This is the reason why innovation in the financial field, such as a complete rewrite of the mechanics of decentralized digital currencies, brings into question new concerns and new security challenges. Recent developments show that designing a decentralized trust-less system means facing not only technical challenges but also user behavior patterns and fundamental economics of money.

2. Security concerns of financial infrastructures

Through their contribution to the functioning of the society and the potential impact in case of a failures, information systems are critical infrastructures if not essential parts of systems that constitute critical infrastructures. In the contemporary economy, many financial instruments are a manifestation of the cyber phenomena, and in addition to intrinsic financial properties, have relevance in a wider sense, given the depth of the interconnectivity of systems. The concept of "money" itself can be regarded in such a manner. It encompasses a fundamental system for a medium of exchange and measure of value in an economy and is heavily relying on a cybernetic infrastructure. New forms of

currency or assets discard the relevancy of a physical medium. Traditionally, the association between any physical assets, specifically the ownership of the asset, and the owner, be it person, corporation, state, etc., is information stored digitally and acknowledged by the rest of society through the validation of a third party. More often, theft itself is completely digital as physical alienation of property is less relevant given the fact that value and wealth are digital. The whole concept of traditional theft becomes insufficiently relevant to describe phenomena that generate financial losses. A cybernetic world has flaws that can be exploited to "legitimate" theft or make it undetectable by the society.

This cyber security crisis can be attributed to a mismatch between cyber threats, their way of developing and activating and solutions developed to combat and resolve vulnerabilities in their systems. Thomas J. Mowbray admits in his book that the problem is not technology itself but man and identifies the specific patterns that generate, often unjustified cyber security risks. Thus, he challenges the conventional thinking and highlights a number of irregularities in security systems:

- The protection systems against malicious software (Malware) is based on the detection of specific code signatures in files. No matter how efficient and fast would the signature databases be updated, fixed protection systems cannot cope with such polymorphic threats. Even a minor change in the code of a virus makes the signature no longer recognizable. Detection systems based on signatures could be replaced by mixed solutions that take into account the reputation of the source program, software behavior, identification of abnormal variations in programming code and other techniques that are based on similarities between codes.
- Processes and mechanisms of certification and accreditation security systems are also a subject of criticism for not representing a protective mechanism against real threats. Certification is the assessment and testing of a system through which vulnerabilities are identified. Accreditation is an executive system approval process that accepts the risks identified in the certification process. The value of accreditation depends, thus on the soundness of test process. Moreover, a number of certifications addressed to professionals in the security sector refer to skills to communicate with management, without covering, in fact, cyber threats. These mechanisms provide security "on paper" and creates a false sense of safety.
- The issue of standards in IT security, consisting of procedures and guidelines for systems architecture have proven to have limited efficiency due to a large volume of information and because it is difficult to implement them in practice without an advanced level of automation enabling management and application requirements standards. Standards also are not updated as quickly emerging threats, and this systemic sync mismatch deepens their inefficiency.

In analyzing cyber security infrastructure a series of behavioral phenomena should be considered, some of which affect technical operating parameters.

- The lack of user awareness on risks and exploitation of erroneous decisions cannot be avoided without an organization-wide educational program.
- Failure to update applications leads to the propagation of known software problems which generates costs to both the client's organization and the developer which must allocate resources for assistance.
- Network operation centers have monitoring systems that logs events or alarms, but some attacks can circumvent alarm systems or are simply ignored by human operator.
- Some technologies behind networks and even the Internet, were not designed to respect principles of security, leading to symptoms and consequences such as lack of authentication for servers or clients, lack of monitoring for malicious packets or

protocols. The solution in this situation is a set of actions and best practices as well as careful configuration of the systems with the installation of security features.

- Another problem is the transition from software installed on the client terminal to online platforms and interfaces exclusively using the Internet. For critical applications and infrastructure, including power plants control systems, this practice creates vulnerabilities with severe implications. SCADA systems (Eng. Supervisory Control and Data Acquisition) underlying machine control, utilities and industrial equipment, are and were very specific targets for attacks.
- Concerns for security is not a priority given the pressure to develop a system or a software product. Security is always an additional cost and result in delays, which affect competitiveness in the short term.

One aspect often treated in the literature on cyber security is the low level of preparedness in front of cyber-threats and conditions conducive to the spread and intensification of attacks. The vulnerabilities are equally apparent for individuals and for companies or governments and the range of threats intensify and diversify. Unlike traditional conflicts, "the enemy" is more difficult to identify because it is not a well-defined group of people or a country. It can sometimes be a company that deploys a cyber-attack to a competitor. The gravity of the situation is amplified by information asymmetry between attacker and victim, who often lacks even the necessary knowledge to understand the technical characteristics of the attack. Also, although the agenda of governments to provide programs to increase the level of preparedness against cyber-attacks, the reality is, in a best case scenario, difficult to assess.

There are numerous cyber security application to financial instruments or systems, but the rise of decentralized digital currencies and assets as a technology and as a possible infrastructure for financial operations has brought up new aspects. Currency as infrastructure has evolved constantly in society and these new forms of digitization an area that deserves analysis. Decentralizing a currency, or eliminating the need for a trusted third party is in itself a security challenge, and solutions to this problem can prove useful elsewhere.

3. Decentralizing and securing a digital currency

Currency as infrastructure is a system in which money is a medium of exchange for an economy, and at the same time a form of evaluation and storage of value. Money, as an instrument, evolved from a physical form with intrinsic value (mostly rare metals) in a physical form without intrinsic value but with a fixed value based on the fixed quantities of precious metals, and then to form of legal tender, a form recognized by law to be a valid method to pay a financial obligation. The concept of currency is closely linked to the nation-state, and to national identity, but regionalization and globalization processes have moved evolutionary trend towards consolidation of markets. The modern system, even if its use is less closely linked to a specific nation, is still a system based on trust in the fundamental institutions (such as central banks) and their management as well as on guarantees offered by governments. Switching from a trust-based digital currency regulated and controlled in a centralized way to a trust-less decentralized digital currency based on a fixed mathematical algorithm and controlled by all users is a profound paradigm shift similar to the invention of the Internet. A significant contribution to this change is trust. Currency traditionally depends in operation and use on trusting third parties, essentially a system that acts as intermediaries through financial institutions and organizations, while decentralized digital currency proposes a system whereby transactions can be made avoiding the need for trust in a third part. The paradox is that this trust-less system still requires trust in the overall technology and user base that allows the

functioning of the system, and that is because value of a currency is still an element of human perception to assign a quality to an abstract concept. The real usefulness of such a technology is difficult to predict, but new ways in which we store and transfer assets, as well as smart contracts are being developed, providing models, or rather infrastructures for a medium of exchange, unmanaged by governments and based on users.

In a conventional financial system the value is represented in ledgers (databases) managed by the financial institutions in which confidence is placed. "Bitcoin" is the most popular currency that does not depend on trust in a third party, and the first that generated a change of perspective in the financial world. Judging by the reactions of governments and financial institutions, bitcoin has become a multifaceted phenomenon combining advances in technology, financial innovation and even issues such as regulation, acts of fraud or new cyber security concerns. Moreover, starting from Bitcoin, new platforms have been developed that bring innovative elements, some benefitting from commercial successes, although such technologies are clearly in their infancy.

The concept behind the emerging digital currency is a decentralized monetary system that does not rely on an institution or a person but on a free and open source software (source code is publicly available to everyone) based on an idea and a set of algorithms. The core of this technology is a distributed permission-less database (the "block-chain") that contains all transactions made in the past as well as current holders of the funds. A transaction is authorized using a private key held by the user which then transmits the transaction message to the network which checks it and includes it in the ledger. The security of the system and all messages is assured through cryptography. This system shows absolute transparency - database, or registry can be questioned by anyone is visible every transaction, every address and associated balance, but identity is hidden behind an address. That does not mean that Bitcoin is an anonymous system, but a pseudonym, because there are situations where the identity of the holder can be induced from an address.

A conventional currency is issued by a governmental body and accepted as a medium of exchange by social convention. As governments have short-term financial interests that generate incentives to increase the money supply, system administration is done by central banks, semi- independent institutions managing monetary policy. However, the traditional currencies are mostly in a long-term trend of inflation. In the case of decentralized systems software creators set network parameters from the beginning, so monetary policy is much simpler. In the case of Bitcoin, the monetary base is fixed and the issue of new currency is made after planning (for example at regular intervals), the new coins being paid to the users that allocate computing power for assuring network security. Unlike a centralized currency where monetary policy decisions are taken by a select group of individuals, in a decentralized network changes can be made only by consensus or at least the desire of the majority. Even with majority support, network changes are difficult to implement if there is opposition from a strong minority leading to the risk division and separation of the currency in two. The immediate advantage is that the system changes that are not in the interest of the majority of users are rejected.

Technical details such as algorithms, programming, operation of networks, cryptography concepts behind security system are extensively documented and freely accessible. This paper does not aim to present these issues, in turn will address features of differentiation from classic monetary systems, advantages and disadvantages and possible applications, including some in the field of critical infrastructures.

A fundamental feature of a decentralized system is that its evolution is independent of any institutional initiative, and, as such, an area where innovation can happen and ideas tried out without permission. Obviously there are associated risks as without a trusted third

party, the responsibility belongs exclusively to the user. Incidentally Bitcoin infrastructure as well as other similar systems or derivatives are designed primarily to ensure security and resilience to attacks. In this case network users are using computational power to solve mathematical problems in order to verify transactions and secure the ledger. In exchange they are rewarded with a fixed amount of currency issued at fixed intervals (at time of writing 25 Bitcoin every 10 minutes), as well as fees from each transaction processed. Participants who runs problem-solving algorithms are called miners. The difficulty of the mathematical problems is automatically adjusted according to the total computational power of the network to maintain the fixed interval.

Users manage their money using an electronic wallet containing access keys, or electronic signatures to access the balance of certain addresses. The coins are stored in the registry, associated public addresses, and each address has a private key without which no transaction can be authorized. Thus, if the coins themselves cannot be stolen or lost access keys can be. In the case of loss, the coins are lost forever while in the case of theft the identity of the thief cannot be acquired using the address. Identity can be inferred by analyzing behavior of a user and linking his or her actions, but this is difficult to do in practice. There are alternative services or currencies offering complete anonymity with untraceable link between the originator and the beneficiary of a transaction. Moreover, any transaction is irreversible once it has been properly signed and included in the ledger. The system itself places the entire responsibility to the individual user who needs to ensure the security of the wallet. Bitcoin addresses algorithm links a private key to a public key which is found on the network, and programs that do this automatically using random number generators that make private key decoding knowing only the public key extremely difficult. Users can also use passwords to generate public addresses, for which decoding computational power required is much smaller. It has been proven that the attackers permanently scan the network for addresses with personal passwords and steal the associated funds.

Another major problem generated by this system is the fact that the ledger itself on which the protocol registers the transaction needs storage space. As the system gets used extensively, the required resources on the network it will become a problem for the users, mainly storage space, electricity and processing power. At the time of writing, the system can manage up to 7 transactions per second, much less than other payment systems that manage up to 2000 transaction per second. This is due to the existing programming language that entails a 1MB limit for a transaction block, a limit that is reached on several occasions during a day. Already storage space has become a problem for which there is no consensus and new technology is needed to support the system and also a rewarding mechanism for the nodes (users of the network) that allocate their storage to store the database. The problem of bitcoin scalability and future sustainability while maintaining decentralization is a much debated topic in this community. The controversy arises from the proposal to increase the block size to accommodate for more transactions per second. Without off the block-chain solutions for clearing transaction, this presents itself as the most obvious choice to allow for more transactions per second, the network will use more resources, information propagation will be slower and fees will increase. Additionally, many argue that operating larger block will encourage only the large miners to be feasible which damages decentralization and weakens the value proposition of Bitcoin. Even though consensus has not been achieved yet, there are several proposals to solve this problem and the security implications. Alternative systems such as Ethereum already experiment with technologies that allow for much better scalability, addressing the limitations of Bitcoin.

Another problem of the system is the way of getting "coins" by new users, as new participants face the economic and technologic barriers. At this moment, at a relatively early phase of the system, access to bitcoin units can be made through:

1. A direct transfer from an owner to a designated address.
2. "Mining", which is the process of allocating computer resources in order to solve mathematical problems to secure the network. This method is no longer a reasonable one because this is done professionally by expensive ASICs - Application Specific Integrated Circuit (a chip for specific applications, in this case, designed to make only one operation – rolling the verification algorithms for the transactions signatures), equipment that becomes outdated very fast, given the growth of the total computer power of the network. When the computing power of one lags behind by the rest of the network, the probability of identifying a transaction block and getting a reward gets smaller. Also if we take into consideration the delivery time of the ASIC units, their cost and the cost of the electricity consumed it is possible to be very difficult to get return on their investment. Even if this is theoretically a market with a perfect competition, because the active users have no mechanism to stop new ones from entering the market, the volatility of the price and also the value of the reward will determine the stabilization of the computing power growth rhythm to cover the incremental operating costs. A new major technology producer or the appearance of a revolutionary technology could produce shocks in the systems. Another restriction of the "mining" system is given by the limited functionality of the ASIC equipment which are designed and built to execute only one operation – security verifications. If the equipment becomes obsolete and their function isn't efficient or the currency simply implodes for one reasons or another, them all this hardware cannot be repurposed for other computing tasks. There are systems proposals that use computing power to participate at scientific projects as an alternative to solving the security algorithms, bringing added value beside the simple security but other problems appear: checking the result must be confirmed quickly. Many scientific projects are difficult to check which encourages some of the miners to present false results in order to get the reward.
3. Exchanging fiat currency to a convertible coin on a specialized market, similar with the FOREX market. This method introduces the risk of trusting a third party because both the money and the coins are held in the accounts of an operator. In the case the operator loses funds due to a cybernetic attack, theft or fraud, the coins can't be recovered. This is not just a theoretical scenario, it has happened several times, the most significant case being the company Mt. Gox, which at a certain moment was managing over 80% of the market trades. In 2014, it stopped the trading and declared bankruptcy, accusing the missing of 850.000 bitcoins (7% of the supply at that time), the equivalent of $ USD 473 million.

However, the Bitcoin kept its users support because the problems were caused by users and not by the system, especially since alternative coins have appeared that use different algorithms and have several applications (Ethereum, Litecoin, Ripple). A defining characteristic of these systems is the network effect, namely the growth in demand as a result of the growing number of the users. From this point of view an entire competitive market between different technologies has been created, with technologies competing for users, liquidity and capitalization. At this level of development, the liquidity on the exchange markets and the daily volume of transactions represent the indicators of the economic manifestation of the network effect.

4. Decentralised financial applications and their security

These technologies have opened the way to a series of applications beyond the storage and transfer of funds with really small costs. The algorithms allow for more

complex transaction through multiple signature, automated payment systems, smart contracts, micro transactions or independent agents – programs that operated without constant human interventions. Some of the possible applications for the infrastructure are described beneath:

a) Digital assets actively connected to physical assets. The Bitcoin infrastructure can be used for the storage of information in a wider sense, and through technologies with multiple access keys tangible assets could be operated (including public infrastructure or industrial applications). Additionally ownership transfer could be done just having simultaneous access to the digital asset and the tangible one.
b) Settlement systems for different financial assets and automatized transfers like bond coupons or dividends. The balance of the portfolio is registered at a public address and the transfer of a dividend or a coupon can be done directly by the issuer using a private signature.
c) The issue of securities directly by the issuers without the processing of an intermediary. If the issuer is trustworthy than public offerings can be done directly by some exchange platforms with significantly smaller costs than through traditional channels.
d) Micro transactions. These applications are appropriate for small payments, for example the access of Internet traffic billed consumption or publications that charge on a per article basis. Another application could be in public transport by charging the travelers only the travelled distance, as well as other benefits such as monitoring the traffic in an anonymous way and to optimize the routes and to allocate resources in order to reduce the operator's costs.
e) Autonomous agents that operate services (usually online services as web hosting, sharing computational power or decentralized money changers) and make payments and cash in, they commit and de-commit contracts. These programs are financed at start-up and can be multiply if profitable. There are certain difficulties in implementing these systems, mostly legal recognition problems, regulation but also security against attackers.
f) Accessible financing solution as crowd-funding. These financing methods invite the final users to support financially a project or an initiative. In the protocol can be programmed a function regarding the finalization of the financing transactions only if the target was achieved, eliminating in this way the need of a centralized agency which can assure the contract. The infrastructure allows also financing some small organizations which wouldn't have access to funds otherwise.
g) Decentralized exchanging markets. In a centralized market the operator gets the orders from the participants and a sorting algorithm that works on the principles of an auction settles the selling orders with the buying ones. In a decentralized marked the participants make their offers public in the distributed register and the registering protocol fits the orders.
h) The escrow deposits with multiple signatures or different complex rules. O entire amount of financial and adjustment contracts of some operation or sequential tasks can be realized by programing them. The advantage compared with traditional financial institutions is given by the much reduced costs.

Even if there is a wide sphere of applications which offer significant advantages regarding the costs or the operating time compared with the classic coin, the architecture itself of the system and the security implemented in the source code makes other applications to be more difficult to realize. Because the transactions are irreversible and from the technical point of view the decentralized digital coins can't be confiscate, giving credits is a risky and difficult operation. At the time of writing this paper there are

operational a certain number of services operators in meeting the demand of credits with the offer, the loans being given directly by the investors to the borrowers according to their reputation. However there isn't a certainty in case of bankruptcy and there is very easy for someone to falsify his identity and to refuse the repayment of the loan. Even more it is very difficult to identify the pyramid schemes which generate very easy positive reputation because the debts are paid from the new credits, until the system makes implosion.

Ultimately, like any other technology, the bit coin also can be overcome by the development of others technologies. The entire security system is based on difficult problems from computing point of view (the factorization of integers, the elliptic curve logarithms etc.), even though it isn't actually prove their difficulty, but the supposed one and the observed in practice one. The quantic computers for example could realize calculations so fast that would invalidate completely the security system which represents o problem not only for the digital decentralized coin but for internet security. There must be developed new techniques of cryptography of public addresses in order to eliminate eventual abuses and attacks using new emerging technologies.

Reaching a higher level of security for the communication on the internet implies implementing some systems that uses protocols resilient to attacks. An example is the exchange protocol of Diffie Hellman cryptographic keys which allows that two users to generate o common key even in the presence of an attacker which can observe uncensored the entire communication between them. An analogy is presented in the diagram below:

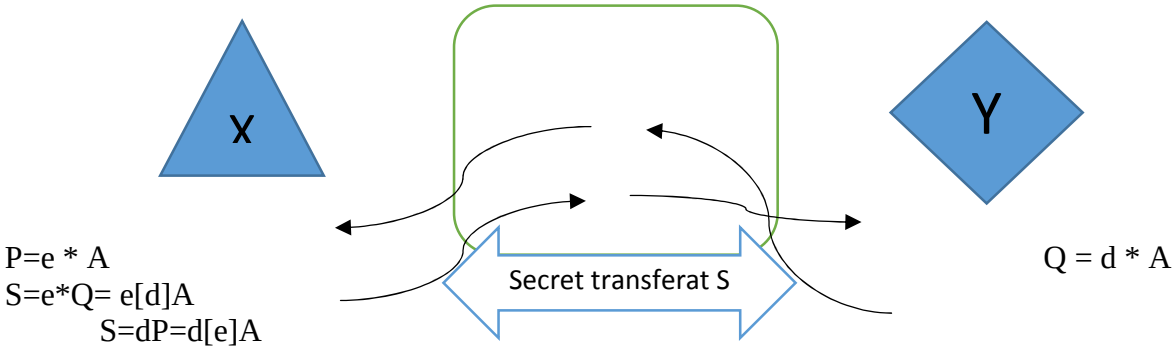

Figure no. 1. Creating the exchange of a Diffie Hellman cryptographic key

Source: Pedro Franco – Understanding Bitcoin, Wiley, p.218

In the figure from above there is presented by a graphic in a simplified manner the following processes: the user X generates a secret key e and calculates a public key P= e*A, where A is the generator of an elliptical curve. The user Y generates a secret key d and calculates o public key Q=d*A which is sent to the user A. The decryption of the secret is made by using simultaneously the private key and public key also, and an attacker which has access to all the transmitted information can't decode the message.

The issue of the decentralized virtual coins wasn't ignored by the financial institutions including investments banks or funds that invest in bit coin, especially central banks and authorities which have identified the need of regulation. In some countries like Russia, Island or Vietnam the use of bit coin has been declared illegal, even though there are limited in instruments by which a this type legislation can be applied. A Central European Bank Report from 2012 reflects the relevance of what they name "virtual coins scheme" for the central banks regarding the establishment of market prices, of the financial systems and of the payment systems and gets to the following conclusions:

The virtual coins scheme:

- do not affect the stability of the prices as long as the money creation continues to remain at a low level;
- they tend to be inherently unstable, but do not put in danger the financial stability, given the limited connection with the real economy and small amount of transactions;
- there aren't regulated and supervised carefully by the public authorities (at that date), even though the participants are exposed at credits, liquidity, operational and legal risks;
- they can represent a test for the public authorities because these can be used by criminals in order to finance illicit activities or for money laundering;
- they can have a negative impact on central banks reputation in the context of a significant growth of the use and the perception on an incident as being central bank's responsibility;
- there are the responsibility of the central banks regarding the specific characteristics of the payment systems.

The same report shows that even though there can be identified many risks regarding the use of these schemes there are positive aspects and financial innovation and that there is a certain expectation regarding the growth of the use in the future which can be encouraged by factors like easy access to the internet, the growth of the share of electronic commerce and services which represent an ideal platform of implementing these payment solutions, low transaction costs, efficient adjustment mechanism of the transactions and also a high level of anonymity. Any evaluation of the risk depends mainly on the size use, being necessary periodic re-evaluations.

5. Future developments and conclusions

Bitcoin is yet to be a mainstream payment system, but it offers a valid argument for an alternative to traditional mechanisms. While transacting directly and securely, without an intermediary is a very attractive proposition, the network has reached a critical mass of users that keeps it relevant but at the same time challenges future scalability. With consensus apparently difficult to achieve and several challenges not yet overcome, many have rushed to declare bitcoin a failed experiment. In reality bitcoin is a successful experiment, but might not be a successful long term currency solution. Many applications have spun off this technology that can prove useful in many areas, including finance.

Among the most visible developments parallel to Bitcoin is the Ethereum project, which proposes an alternative way of providing a similar level of verification that Bitcoin provides while offering a solution for smart contracts and applications that benefit from decentralized validation from the network. At the time of wiring the market capitalization of Ethereum is about one billion euro, or sixth of Bitcoin, the only alternative currency comparable in scale to Bitcoin. This technology has gained a lot of attention due to being a platform for large banks to investigate smart contracts and financial applications such as bonds. Smart contracts are programs that facilitate automated performance and can be implemented to use the computational power of the Ethereum network. The purpose is to use a shared global infrastructure that can store and move value, as well as represent ownership of property with the validation of the entire network. Developers can create ad-hoc markets, store registries of debt or promises (solving the shortcoming of irreversible bitcoin operations), move funds in accordance to instructions from the past all without intermediaries and counterparty risk.

To conclude, we consider that decentralized solution for currencies, assets and smart contracts to be one of the most important economic and social developments of the past

years. While we are not yet ready to declare bitcoin as a dead currency, it is clear that alternative systems and specific applications have gained a lot of traction lately and bitcoin no longer dominates the overall share of this niche market. Even so, on the market bitcoin has behaved like gold on several occasions, acting as an asset bought to protect savings against adverse conditions, inflation or other financial risks, and certainly provides a solid step forward towards the complete free market that even Friederich von Hayek envisioned in his book "Denationalisation of Money: The Argument Refined".

References

1. Arvind, N., Joseph, B., Edward, F., Andrew, M. and Steven, G., 2016. *Bitcoin and Cryptocurrency Technologies.* Princeton: Princeton University Press.
2. Blundell-Wignall, A., 2014. *The Bitcoin Question Currency versus Trust-Less Transfer Technology.* OECD Publishing. Available at: <http://dx.doi.org/10.1787/5jz2pwjd9t20-en>.
3. Brito, J. and Castillo, A., 2013. *Bitcoin a Primer for Policymakers.* Arlington: Mercatus Center, George Mason University.
4. Carayannis, E.G., Campbell, D.F. and Efthymiopoulos, M.P., 2014. *Cyber-Development, Cyber-Democracy and Cyber-Defense - Challenges, Opportunities and Implications for Theory, Policy and Practice.* New York: Springer.
5. Ethereum, 2016. *Ethereum Homestead Documentation.* [on-line] Available at: <https://ethereum-homestead.readthedocs.org/en/latest/>.
6. European Central Bank, 2012. *Virtual Currency Schemes.* Germany: Frankfurt.
7. Franco, P., 2015. *Understanding Bitcoin - Cryptography, Engineering and Economics.* UK: John Wiley & Sons Ltd.
8. Gordon, K. and Dion, M., 2008. *Protection of 'Critical infrastructure' and the role of investment policies relating to national security.* Paris: Organisation for Economic Cooperation and Development.
9. Shaughnessy, H., 2015. *Shift - A user's guide to the new economy.* London: The Disruption House.
10. Singer, P. and Friedman, A., 2014. *Cybersecurity and Cyberwar -What everyone needs to know*. New York: Oxford University Press.
11. Yonatan, S. and Aviv, Z., 2013. *Accelerating Bitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains.* Israel Science Foundation.